WHAT IS CLAIMED IS:

1. A method for generating a code to be embedded in a predetermined content, comprising the steps of:

calculating a plurality of residues, taking a plurality of integers which are relatively prime to each other, as moduli, with respect to a user identification number of a user who uses the content;

generating a plurality of component codes respectively expressing the residues obtained in the residue calculating step; and

concatenating the component codes generated in the component code generating step, thereby to generate the code to be embedded.

2. A unit for generating a code to be embedded in a predetermined content, comprising:

residue calculating means for calculating a plurality of residues, taking a plurality of integers which are relatively prime to each other, as moduli, with respect to a user identification number of a user who uses the content;

component code generating means for generating a plurality of component codes respectively expressing the residues obtained by the residue calculating means; and

concatenating means for concatenating the component codes generated by the component code generating means, thereby to generate the code to be

embedded.

3. A unit according to claim 2, wherein the component code generating means generates, as the plurality of component codes, codes each constructed by continuous sequences of 1 and 0, taking a predetermined number of bits as a unit.

4. A method for detecting an embedded code which is embedded in a predetermined content and concatenates a plurality of component codes, comprising the steps of:

dividing the embedded code into the plurality of component codes;

decoding each of the component codes divided, thereby to obtain a plurality of residues pairs each comprising two residues, taking a plurality of integers which are predetermined and are relatively prime to each other, as moduli; and

calculating a user identification number of a colluder who made a collusion attack on the content, from the plurality of residue pairs, wherein

the plurality of component codes are component codes that have a possibility to have a method of decoding at least one of the residues with respect to the user identification number of the colluder.

5. A unit for detecting an embedded code which is embedded in a predetermined content and concatenates a plurality of component codes, comprising:

code dividing means for dividing the embedded code into the plurality of component codes;

component code decoding means for decoding each of the component codes divided, thereby to obtain a plurality of residues pairs each comprising two residues, taking a plurality of integers which are predetermined and are relatively prime to each other, as moduli; and

colluder number calculating means for calculating a user identification number of a colluder who made a collusion attack on the content, from the plurality of residue pairs, wherein

the plurality of component codes are component codes that have a possibility to have a method of decoding at least one of the residues with respect to the user identification number of the colluder.

6. A unit according to claim 5, wherein the plurality of component codes are each constructed by continuous sequences of 1 and 0, taking a predetermined number of bits as a unit.

7. A unit according to claim 5, further comprising collusion determining means for determining presence or absence of a collusion from the plurality of residue pairs, wherein the colluder identification number calculating means calculates the user identification number of the colluder, if presence of a collusion is determined by the colluder determining

means.

8. A unit according to claim 5, wherein the colluder number calculating means includes:

a residue selecting section for selecting one residue from each of k' inputted residues pairs, thereby to generate a set of k' residues (R1, R2, ···, Rk');

a Chinese remainder theorem section for calculating a candidate of a user identification number u of a colluder, from k residues (S1, S2, ···, Sk) which are different from each other and selected from the set of k' residues generated by the residue selecting section, in accordance with a Chinese remainder theorem; and

a consistency checking section for selecting the k residues from the set of k' residues generated by the residue selecting section, for supplying the k residues to the Chinese remainder theorem section, for specifying a user identification number of the colluder from the candidate of the user identification number u of the colluder calculated by the Chinese remainder theorem section, and for outputting the user identification number of the colluder, wherein

the consistency checking section has selection processing for selecting the k residues from the set of k' residues generated by the residue selecting section, determination processing for determining whether or not

a relationship of Ri=u mod pi ($i=i_1, i_2, \cdots, i_\ell$) exists between the candidate of the user identification number u of the colluder calculated by the Chinese remainder theorem section and a predetermined number (ℓ) of residues among remaining (k'-k) residues, and output processing for outputting the candidate as a user identification number of a colluder if the relationship exists as a result of the determination processing,

if the relationship does not exist, a new combination of k residues (S1, S2, ···, Sk) is selected from the set of the k' residues generated by the residue selecting section, thereby to carry out the determination processing, and if the relationship does not exist with respect to any of all combinations of k residues (S1, S2, ···, Sk), a new set of k' residues is requested to the residue selecting section, and the selection processing and the determination processing are repeated until the relationship exists.

9. A unit for generating a code to be embedded, comprising:

calculating means for calculating a set of a plurality of integral elements in correspondence with an inputted user identification number;

component code generating means for generating component codes respectively in correspondence with the integral factors, such that among k' component codes capable of expressing all sets of integral elements

that are calculated by the calculating means with respect to a predetermined number of user identification numbers, k combinations of the k' component codes can uniquely express the user identification numbers; and

concatenating means for concatenating the component codes generated by the component code generating means, thereby to generate a code to be embedded, wherein

k' is determined to be $c(k+\ell)/q$ or more where c is a positive integer of 3 or more, ℓ is a positive integer, and q is a number of the integral elements which can be detected from each of the component codes when detecting the embedded code.

10. A unit according to claim 9, wherein, where p_i (i=1, 2, ···, k') is a number of values which each of the integral factors calculated by the calculating means can take with respect to the predetermined number of user identification numbers and where ε is a detection error rate which is assumed when detecting the code to be embedded, k' is determined such that a condition of

$$\left[1-\prod_{i=1}^{l}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+l)/2 C_{k+l}\times 2^{k+l}} \geq 1-\frac{\varepsilon}{2}$$

is satisfied.

11. A unit according to claim 9, wherein the calculating means calculates a set of residues, which

take a plurality of integers relatively prime to each other as moduli, as the set of integral elements, in correspondence with the inputted user identification number.

12. A unit according to claim 9, wherein the calculating means calculates a set of numbers of elements, which belong to an equivalence class defined by a parallel transformation, as the set of integral elements, in correspondence with the inputted user identification number.

13. A unit according to claim 9, wherein the calculating means calculates a set of numbers of elements, which belong to an equivalence class defined by a parallel transformation, as the set of integral elements, in correspondence with the inputted user identification number, and

where p_i (i=1, 2, ···, k') is one same positive integer p, a condition of

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p - 1}$$

is further satisfied.

14. A unit for detecting an embedded code, comprising:

code extracting means for extracting an embedded code from a target in which the embedded code is embedded, the embedded code concatenating component codes respectively generated in correspondence with an inputted user identification number and also being such

that among k′ component codes capable of expressing all sets of integral elements that are calculated with respect to a predetermined number of user identification numbers, k combinations of the k′ component codes can uniquely express the user identification numbers;

code dividing means for making a division into extracted component codes;

component code decoding means for decoding each of the component codes divided; and

colluder number calculating means for calculating a user identification number of a colluder from a decoding result of each of the component codes, wherein

k′ is determined to be $c(k+\ell)/q$ or more where c is a positive integer of 3 or more, ℓ is a positive integer, and q is a number of the integral elements which can be detected from each of the component codes when detecting the embedded code.

15. A unit according to claim 14, wherein, where p_i (i=1, 2, ···, k′) is a number of values which each of the integral factors calculated by the calculating means can take with respect to the predetermined number of user identification numbers and where ε is a detection error rate which is assumed when detecting the embedded code, k′ is determined such that a condition of

$$\left[1-\prod_{i=1}^{l}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+l)/2 C_{k+l}\times 2^{k+l}} \geq 1-\frac{\varepsilon}{2}$$

is satisfied.

16. A unit according to claim 14, wherein the set of integral elements is a set of residues, which are calculated in correspondence with the user identification number and take a plurality of integers relatively prime to each other as moduli.

17. A unit according to claim 14, wherein the set of integral elements is a set of numbers of elements which are calculated in correspondence with the user identification number and belong to an equivalence class defined by a parallel transformation.

18. A unit according to claim 14, wherein the set of integral elements is a set of numbers of elements which are calculated in correspondence with the user identification number and belong to an equivalence class defined by a parallel transformation, and

where p_i (i=1, 2, ···, k') is one same positive integer p, a condition of

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p-1}$$

is further satisfied.

19. A unit for detecting an embedded code, comprising:

code extracting means for extracting an embedded code from a target in which the embedded code is embedded, the embedded code concatenating component codes respectively generated in correspondence with an inputted user identification number and also being such

that among k' component codes capable of expressing all sets of integral elements that are calculated with respect to a predetermined number of user identification numbers, k combinations of the k' component codes can uniquely express the user identification numbers;

code dividing means for making a division into extracted component codes;

component code decoding means for decoding each of the component codes divided; and

colluder number calculating means for calculating a user identification number of a colluder from a decoding result of each of the component codes, wherein

the component code decoding means includes a block dividing section for dividing each of the component codes into blocks, a counting section for counting a number of bits of "1" in every one of the blocks, a first determining section for determining whether or not a count value obtained by the counting section exceeds a first threshold value, a second determining section for determining whether or not the count value is smaller than a second threshold value, a minimum position selecting section for selecting a minimum block determined as exceeding the first threshold value by the first determining section, and a maximum position selecting section for selecting a maximum block determined as being smaller than the second threshold value, thereby to output a selection results

of the minimum and maximum position selecting sections, as a decoding result.

20. A unit according to claim 2, further comprising user identification number assigning means for selecting one candidate that is erroneously detected as the user identification number of the colluder at a smaller possibility, among a plurality of user candidate number candidates, in response to an assigning request for the user identification number, and for assigning the selected user identification number to user specifying data which specifies the user.

21. A unit according to claim 20, wherein the user identification number assigning means inputs sequentially the plurality of user identification number candidates one after another, determines whether the possibility at which each of the candidates is erroneously detected as the user identification number of the colluder is high or low, and assigns a candidate to the user specifying data at a time point when a user identification number candidate having the possibility is determined to be low is inputted.

22. A unit according to claim 20, wherein the user identification number assigning means includes storage means which stores a plurality of user identification numbers having a lower possibility at which the plurality of user identification numbers are

erroneously detected as the user identification numbers of the colluder, and selects and reads a user identification number to be assigned to the user specifying data from the user identification numbers stored in the storage means.

23. A unit according to claim 5, wherein the colluder number calculating means generates at least one user identification number candidate having a possibility to be the user identification number of the colluder, from the plurality of residue pairs, selects at least one user identification number having a lower possibility to be erroneously detected as the user identification number of the colluder, among the candidate, and decides the selected user identification number as the user identification number of the colluder.

24. A unit according to claim 5, wherein the colluder number calculating means sequentially generates a plurality of user identification number candidates having a possibility to be the user identification number of the colluder, from the plurality of residue pairs, determines whether a possibility to be erroneously detected as the user identification number of the colluder is high or low, with respect to the candidates, and decides all of user identification numbers that have the possibility determined to be low, as user identification numbers of

colluders.

25. A unit according to claim 23, wherein the colluder number calculating means obtains a number of those residues among all of the residues pairs that satisfy a congruence to the residues taking the plurality of integers as modulus, with respect to all user identification numbers, and generates a user identification number which makes the number to be a predetermined threshold value or more, as a user identification number candidate of the colluder.

26. A unit according to claim 24, wherein the colluder number calculating means obtains a number of those residues among all of the residues pairs that satisfy a congruence to the residues taking the plurality of integers as modulus, with respect to all user identification numbers, and generates a user identification number which makes the number to be a predetermined threshold value or more, as a user identification number candidate of the colluder.

27. A unit according to claim 5, wherein the colluder number calculating means includes storage means which stores a plurality of user identification numbers having a lower possibility at which the plurality of user identification numbers are erroneously detected as the user identification numbers of the colluder, and decides a user identification number which coincides with at least one user

identification number candidate having a possibility to be the user identification number of the colluder, generated from the plurality of residue pairs, among the user identification numbers stored in the storage means.

28. A watermark embedding unit for embedding a code to be embedded, which is generated by the unit according to claim 2, as watermark information into the content.

29. A watermark embedding unit for embedding watermark information containing information of a user identification number into a predetermined content, comprising:

means for outputting one codeword selected from a plurality of codewords constructing a simplex code, in correspondence with an inputted user identification number; and

means for embedding the outputted codeword as the watermark information into the content as an embedding target.

30. A watermark detecting unit for detecting watermark information containing information of a user identification number from a predetermined content, comprising:

means for outputting one codeword selected from a plurality of codewords constructing a simplex code, in correspondence with an inputted user identification

number;

means for obtaining a correlation value between the outputted codeword and the content; and

means for determining presence or absence of a codeword corresponding to the inputted user identification number in the content, based on the correlation value.

31. A watermark detecting unit for detecting watermark information containing information of a user identification number from a predetermined content, comprising:

means for outputting a plurality of codewords which respectively correspond to a plurality of previously registered user identification numbers and which construct a simplex code;

means for obtaining a correlation value between each of the outputted codewords and the content; and

means for determining presence or absence of watermark information, based on norm calculated, regarding each obtained correlation value as a vector, and for specifying a colluder based on the correlation value if presence of watermark information is determined.

32. A storage medium which stores a content in which a code to be embedded, which is generated by the unit according to claim 2, is embedded.